Computing the maximal subgroups of a permutation group I

Bettina Eick and Alexander Hulpke

Abstract. We introduce a new algorithm to compute up to conjugacy the maximal subgroups of a finite permutation group. Or method uses a "hybrid group" approach; that is, we first compute a large solvable normal subgroup of the given permutation group and then use this to split the computation in various parts.

1991 Mathematics Subject Classification: primary 20B40, 20-04, 20E28; secondary 20B15, 68Q40

1. Introduction

Apart from being interesting themselves, the maximal subgroups of a group have many applications in computational group theory: They provide a set of proper subgroups which can be used for inductive calculations; for example, to determine the character table of a group. Moreover, iterative application can be used to investigate parts of the subgroups lattice without the excessive resource requirements of computing the full lattice. Furthermore, algorithms to compute the Galois group of a polynomial proceed by descending from the symmetric group via a chain of iterated maximal subgroups, see **[Sta73, Hul99b]**.

In this paper, we present a new approach towards the computation of the conjugacy classes of maximal subgroups of a finite permutation group. For this purpose we use a "hybrid group" method. This type of approach to computations in permutation groups has been used recently for other purposes such as conjugacy classes **[CS97, Hul]**, normal subgroups **[Hul98, CS]** or the automorphism group **[Hol00]**.

For finite solvable groups there exists an algorithm to compute the maximal subgroups using a special pc presentation, see **[CLG, Eic97, EW]**. Our approach incorporates a generalization of this method. Vice versa, if the group in question is finite solvable, then our algorithm reduces to this known method.

For finite groups in general the commonly used approach so far to obtain the maximal subgroup has been via a computation of the full subgroup lattice, see **[Neu60, Hul99a, CCH]**. Our approach in contrast avoids the time and space consuming calculation of all subgroups and thus is not only more efficient but also capable of dealing with much larger groups.

2. Outline

Let G be a finite group and S its *solvable radical*; that is, its largest solvable normal subgroup. Then the factor G/S does not contain any solvable normal subgroups; i.e. it is *fitting free*, and thus the socle $\mathrm{Soc}(G/S)$ is the direct product of nonabelian simple groups.

If G is a permutation group on d points, then we can compute S and a faithful permutation representation of G/S on at most d points **[LS97, Hol97]**. Similarly, given G/S as a permutation group we can compute $L/S = \mathrm{Soc}(G/S)$ and a faithful permutation representation of G/L **[CS, Corollary 2.3]**.

We use these algorithms to determine separately the maximal subgroups of G in the following three families:

I) Maximal subgroups that do not contain S. This is done using a generalization of the solvable group method, see Section 3.

II) Maximal subgroups that do contain S but do not contain L. These groups are preimages of the maximal subgroups of G/S that do not contain $\mathrm{Soc}(G/S)$, see Section 4.

III) Maximal subgroups that do not contain L; i.e. preimages of the maximal subgroups of G/L. Since L is a non-trivial subgroup of G and we have a permutation representation for G/L we obtain these subgroups by a recursive call of the algorithm.

Our algorithm for the first step is very efficient in general. Moreover, the groups G/L as considered in step III) are often solvable and very small. Hence the last step is usually easy for our methods. Therefore, we are left with step II) as the main time-consuming part of the algorithm.

3. The Solvable Radical

We first consider case I) of Section 2 and thus we want to compute the maximal subgroups M of G which do not contain the solvable radical S of G.

Let $S = S_1 \rhd S_2 \rhd \ldots \rhd S_l \rhd S_{l+1} = \{1\}$ the lower nilpotent series of S; that is, S_{i+1} is defined as the minimal normal subgroup of S_i with nilpotent factor group. Furthermore let $S_i^*/S_{i+1} = \Phi(S_i/S_{i+1})$ the Frattini subgroup of the nilpotent factor S_i/S_{i+1}. Then the refined lower nilpotent series

$$S = S_1 > S_1^* \geq S_2 > \ldots > S_l > S_l^* \geq S_{l+1} = \{1\}$$

is a characteristic series of S and hence a normal series of G. Note that this series can be computed effectively by the methods described in **[CLG]**. The factors S_i/S_i^*

are called *heads* of S and they are non-trivial direct products of elementary abelian groups.

In the following lemma we relate maximal subgroups of G with the refined lower nilpotent series and the heads of G. The proof of it for solvable groups in **[Eic97]** will carry over directly also to nonsolvable groups.

Lemma 3.1. *Let M be a maximal subgroup of G with $MS = G$.*

a) M covers all but one of the factors of the refined lower nilpotent series of S. This non-covered factor is a head of S.

b) Suppose that M does not cover the head S_i/S_i^* for some i. Define $N = S_i \cap M$. Then N/S_i^* is a maximal G-normal subgroup of S_i/S_i^*.

c) M/N is a complement to S_i/N in G/N.

Thus for each maximal subgroup M of G with $MS = G$ there exists a unique head S_i/S_i^* which is not covered by M. For each $i \in \{1, \ldots, l\}$ we will separately compute the maximal subgroups which do not cover S_i/S_i^*.

For this purpose we proceed in two steps: First we compute all maximal G-normal subgroups N/S_i^* of S_i/S_i^*. Since S_i/S_i^* is a direct product of elementary abelian p-groups, we may consider each Sylow p-subgroup of S_i/S_i^* separately and compute its maximal G-normal subgroups. This, in turn, can be translated into a calculation of the maximal submodules of a finite dimensional $\mathbb{F}_p G$-module which can be obtained efficiently using the MeatAxe, see **[HLOR95]**.

Then in the second step we consider each of the computed subgroups N in turn and compute the conjugacy classes of complements to S_i/N in G/N. By Lemma 3.1 these are the conjugacy classes of maximal subgroups as desired. To compute the complements we distinguish again two cases. If $i > 1$ and hence $S_i < S$, we can use a very efficient method described in Section 3.2. However, if $i = 1$, this algorithm cannot be applied and we have to determine the complements by a more general and less efficient approach, see Section 3.1.

To simplify notation, we assume from now on that $S_i^* = 1$ and that S_i is an elementary abelian p-group.

3.1. The top head S_1/S_1^*. Recall that $S_1 = S$ and let N be a maximal G-normal subgroup of S as considered in Lemma 3.1.

We wish to compute the conjugacy classes of complements to S/N in G/N. For this purpose we need a finite presentation for G/S. A polynomial length presentation can be obtained efficiently by the methods described in **[BGK+97, KS99]**, since we have a permutation representation of G/S.

If the finite presentation is given, then the calculation can be performed as described in **[CNW90]**. Since S/N is an elementary abelian p-group, this can be reduced to solving linear equations over the finite field with p elements.

Still, the calculation of a presentation and subsequential complement calculation may be time-consuming. In general, there seems to be no better method available, but in the special case when S is central under the action of G we can avoid the computation of a presentation with the following method.

Lemma 3.2. *Let S be a central normal p-subgroup of the finite group G. Furthermore let $R = G'G^p$. Then the maximal subgroups of G which do not contain S are preimages of those maximal subgroups of the elementary abelian p-group G/R which do not contain SR/R.*

Proof. Any maximal subgroup M of G which does not contain S must be normal of index p in G, since S is central, and therefore we obtain $R \leq M$. Thus we can translate the problem to G/R which completes the proof. □

To check the condition of Lemma 3.2, we consider the elementary abelian p-group G/R as a vector space V over the field with p-elements. Then SR/R corresponds to a subspace W of V and we need to find all those maximal subspaces of V which do not contain W.

3.2. The lower heads S_i/S_i^* with $i > 1$. In this case we can determine complements more efficiently than in the case of Section 3.1. In particular, we can always avoid the computation of a presentation of G/S_i^*. We use the following theorem on the head S_i/S_i^* and again we assume that $S_i^* = 1$ and S_i is an elementary abelian p-group. We use the following well-known lemma to prove the main theorem of this section.

Lemma 3.3. *Let G be finite group with normal elementary abelian p-subgroup A and nilpotent p'-subgroup T such that $TA \lhd G$ and $[A,T] = A$. Then $N_G(T)$ is a complement to A in G and all complements to A in G are conjugate.*

Proof. First we show that $N_G(T)$ is a complement to A in G. Let $g \in A \cap N_G(T)$. Then for each $t \in T$ we obtain $[g,t] = g^{-1} \cdot g^t \in A$ and $[g,t] = t^{-g} \cdot t \in T$. Hence $[g,t] = 1$ for all $t \in T$ and thus $g \in C_A(T)$. However, since $[A,T] = A$ and A and T are of coprime order, this yields $g = 1$. Therefore $A \cap N_G(T) = 1$.

Now let $g \in G$. Note that TA is a solvable normal subgroup of G with p-complement T. Thus $T^g \leq TA$ and T^g is another p-complement of TA. Hence $T^g = T^a$ for some $a \in A$. Therefore $ga^{-1} \in N_G(T)$ and we obtain that $AN_G(T) = G$. Hence $N_G(T)$ is a complement to A in G.

Finally let K be an arbitrary complement to A in G. Since $TA \lhd G$, we have that $|TA \cap K| = |TA/A|$ and hence $TA \cap K$ is another p-complement of TA. Thus $TA \cap K$ is conjugate to T. Therefore $K = N_G(TA \cap K)$ is conjugate to $N_G(T)$. □

Now we can apply the above lemma to show the following theorem.

Theorem 3.4. *Let $i \in \{2,\dots,l\}$ and suppose that N is a maximal G-normal subgroup of the elementary abelian p-group S_i. Then there exists exactly one conjugacy class of maximal subgroups M of G with $S_i \cap M = N$. A representative of this class can be computed as $N \cdot N_G(T_{i,p})$ where $T_{i,p}$ is a p-complement of S_{i-1}.*

Proof. Note that in **[EW]** a proof is given for the case that G is solvable. We give an alternative proof which shows the theorem in its more general version.

Let L be an arbitary G-normal subgroup of S_i and consider $A = S_i/L$ and $T = T_{i,p}L/L$. Since A is the last term of the lower nilpotent series of G/L, we obtain that $[A,T] = A$ and hence we can apply Lemma 3.3. This yields that there exists exactly one conjugacy class of complements to S_i/L in G/L.

Thus, for $L = 1$ we obtain that $N_G(T_{i,p})$ is a complement to S_i in G.

Moreover, for $L = N$ a maximal G-normal subgroup of S_i the above argument shows that there is exactly one maximal subgroup M of G with $S_i \cap M = N$. However, $N \cdot N_G(T_{i,p})$ is a complement to S_i/N and thus it is a maximal subgroup of this type. □

Thus instead of computing complements by the standard approach we determine the normalizer $N_G(T_{i,p})$. Again, we do not use the a general method for this purpose, but we introduce a special approach. Note that the existence of a nilpotent p-complement $T_{i,p}$ is crucial for our special method. As there is no such p-complement in G/S_1^*, we cannot apply this method to the top head S/S_1^*, but only to all the lower heads.

3.3. Computing a normalizer of $T_{i,p}$. To simplify notation let $A = S_i$ and $T = T_{i,p}$. Since $N_G(T)$ is a complement to A in G, for every $g \in G$ there exists an element $a \in A$ with $ga \in N_G(T)$. We introduce a method to compute such an element a as solution of a linear equation over $\mathbb{F}_p$. This enables us to compute a generating set of $N_G(T)$ from a generating set of G.

Remark 3.5. The factor TA/A is the p-complement of the nilpotent group S_{i-1}/A. Since S_{i-1}/A is normal in G/A, we obtain that TA/A is normal in G/A, and hence TA is normal in G.

Let $t \in T \leq TA$ and $g \in G$. Then $[t,g] \in TA$ and thus $[t,g] = sb$ for some $s \in T$ and $b \in A$. Note that s and b are unique, since TA is the semi-direct product of the p-group A and the p'-group T.

If $ga \in N_G(T)$, then $[t,ga] \in T$. Since $[t,ga] \equiv [t,g] \bmod A$, we obtain that $[t,ga] = s$ in this case. On the other hand we have

$$\begin{aligned}[t,ga] &= t^{-1}\cdot a^{-1}\cdot g^{-1}\cdot t\cdot g\cdot a\\ &= (a^{-1})^t\cdot[t,g]\cdot a\\ &= (a^{-1})^t\cdot s\cdot b\cdot a\\ &= s\cdot(a^{-1})^{ts}\cdot b\cdot a\end{aligned}$$

Combining the above formulas we obtain

$$[t,ga]=s \quad \text{if and only if} \quad a^{ts}a^{-1}=b.$$

Note that ts acts on A as $t[t,g]=t^g$ and hence the action of ts can be computed easily from t and g. Moreover, the factorisation $[t,g]=sb$ is easy to compute, since b is just the p-part of the commutator $[t,g]$.

Altogether we can compute the element a as solution of the equations $a^{t^g}a^{-1}=b$ where t runs over a generating set of T. Since A is an elementary abelian p-group, we can translate this set of equations into a system of inhomogeneous linear equations over $\mathbb{F}_p$.

4. Fitting-free groups

Now we turn our attention to the maximal subgroups in case II) of Section 2. Thus we want to determine the maximal subgroups of G which contain the solvable radical S, but do not contain L, where L/S is the socle of G/S. Recall that we may determine a permutation represenation of G/S efficiently and hence, without loss of generality, we assume that $S=1$ and G is a fitting free group with socle L.

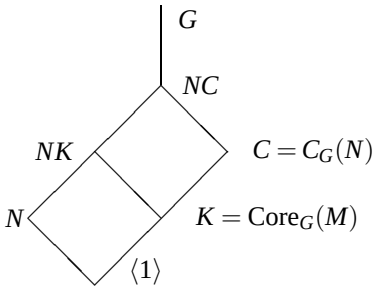
We first compute a G-chief series $L=N_0>\cdots>\langle 1\rangle$ of L, see **[KL90, CH97, Hul]**. We will parametrize the maximal subgroups according to the largest of the N_i they contain. We shall describe this process only for one index, to obtain all maximal subgroups one has to run in a loop over all N_i.

Let M be a maximal subgroup of G with $L\not\leq M$ and let j the smallest index such that $N_j\leq M$. To simplify the notation we assume now that $N_j=\langle 1\rangle$ by translation to the factor G/N_j and we denote N_{j-1} by N. Note that we do not need to construct a faithful representation for this factor group in our algorithm, since all necessary calculations can be performed with representatives for the elements and full preimages of subgroups.

Thus we have reduced to the case that N is a minimal nonabelian normal subgroup of G and we want to determine the maximal subgroups M of G with $N\not\leq M$.

Let $C=C_G(N)$ and $K=\mathrm{Core}_G(M)=\bigcap_{g\in G}M^g\lhd G$. Then $K\leq M$ and therefore $N\not\leq K$. Moreover, $N\cap K=\langle 1\rangle$, since N is a minimal normal subgroup, and thus the normal subgroup K centralizes N. Hence we obtain $K\leq C$ and we can summarize the situation as in the following picture.

Remark 4.1. In this notation we obtain that G/K has a faithful primitive permutation representation on the cosets of M/K and M/K can be described as the point stabilizer of this permutation representation. Thus to determine all maximal subgroups of G not containing N we first compute all possible candidates for the normal subgroup K, then we calculate all faithful primitive permutation representations of G/K and finally we obtain the maximal subgroup M as point stabilizer of the permutation representation.



The structure of the socle of a primitive permutation group can be described in detail. We will use this to determine the structure of G/K more precisely.

Theorem 4.2. *Consider the notation as in the above picture. Then* $\mathrm{Soc}(G/K) = NC/K$. *Moreover, one of the following two cases holds for G.*

A) $K = C$ *and* $\mathrm{Soc}(G/K) = NK/K \cong N$ *is a minimal subgroup of* G/K.
(We say G/K *is primitive of type A.)*

B) $K < C$ *and* $\mathrm{Soc}(G/K) = NK/K \times C/K \cong N \times N$ *is a direct product of two permutation isomorphic subgroups of* G/K.
(We say G/K *is primitive of type B.)*

Proof. First we observe that $\mathrm{Soc}(G/K) = NC/K$. Clearly, NK/K is a minimal normal subgroup of G/K and hence $NK/K \leq \mathrm{Soc}(G/K)$.

Next we observe that $C/K \leq \mathrm{Soc}(G/K)$. This holds trivially if $C = K$. Thus we assume that $K < C$. By definition of K the factor G/K has a faithful primitive permutation representation. Its nontrivial normal subgroups NK/K and C/K centralize each other and both act regularly by **[DM96, Theorem 4.2A]**. Thus C/K is a minimal normal subgroup of G/K and the claim follows.

Now we show that $\mathrm{Soc}(G/K) \leq NC/K$. Let $A \lhd G$ such that A/K is a minimal normal subgroup of G/K. If $N \leq A$, then we obtain $A \leq NK \leq NC$. Otherwise $N \cap A = \langle 1 \rangle$ and thus $A \leq C \leq NC$. Thus we proved that $\mathrm{Soc}(G/K) = NC/K$.

By Theorem 4.3B of **[DM96]** the socle of a primitive permutation group is either a minimal normal subgroup or a direct product of two permutation isomorphic minimal normal subgroups. Applying this to our sitation, we obtain directly that G/K must be of type A or B, proving the theorem. □

Applying Theorem 4.2 we now distinguish the two cases A) and B) on the centralizer C of N in G and its relationship to the core K of the desired maximal subgroup M of G.

To compute all maximal subgroups in type A which do not contain N we compute the action of G on N. The kernel of this action is C and in type A we have $C = K$. Following **[Hul, section 3]** the image Q of this action can be represented as a permutation group of small degree. We then must test whether Q has faithful primitive permutation representations of type A and compute point stabilizers of these representations to determine the desired maximal subgroups. See Section 5 for further details.

To determine the maximal subgroups in type B we first must obtain all all possible kernels $K < C$. Again, we obtain C as the kernel of the action of G on N. Then we intersect the subgroups N_i of the chief series with C and remove duplicates. This yields a series $C = C_0 > C_1 > \cdots > \langle 1 \rangle$ of normal subgroups in C whose factors are G-chief factors.

For every possible K there is a minimal index k with $C_k \leq K$. In this case C_{k-1}/C_k is isomorphic to $C/K \cong N$ and hence C_{k-1}/C_k is nonabelian simple. Thus we obtain $K = C_{C/C_k}(C_{k-1}/C_k)$. In particular, each chief factor of C isomorphic to N can give rise only to at most one possible subgroup K.

To obtain all potential kernels K we loop over the factors C_{k-1}/C_k for all k. If $C_{k-1}/C_k \cong N$, we compute the simultaneous action φ of G on N and on C_{k-1}/C_k. Let Q be the image of this action. If the index of $\ker\varphi = C_{C/C_k}(C_{k-1}/C_k)$ in C is $|N|$, then the socle of Q is a direct product of two normal subgroups isomorphic to N and only in this case φ might give a primitive factor of type B.

If this is the case, we have to test whether Q has faithful primitive permutation representations of type B and to compute the maximal subgroups afforded by these representations. Again, see Section 5.

By the Jordan-Hölder Theorem primitive actions of type B can only arise if there is *another* chief factor N_{i-1}/N_i of G with $i < j$ which is isomorphic to N. This can be used as a quick initial test.

Note, that we do not need to get explicit isomorphisms of the chief factors, but only isomorphism types. However, the isomorphism type of a finite simple group is determined already by the size of the simple group except for $|PSL_3(4)| = |A_8|$ and $|PSp_{2n}(q)| = |P\Omega_{2n+1}(q)|$, see **[Cam81]**; to distinguish between groups of same size one can either consider the size of p-element centralizers or use the approach of **[AB00]**.

5. Primitive Permutation Representations

By the reduction in the previous section we can assume that we have given a permutation group G and we need to determine the faithful primitive permutation representations of G. We know that the socle $H = \mathrm{Soc}(G)$ is the direct product of isomorphic simple groups; that is, $H = T_1 \times \ldots \times T_m$ with $T_i \cong T$ nonabelian simple. We say that H is *homogeneous* and the simple group T is called the *type* of H.

The O'Nan-Scott Theorem **[Sco80]** gives a structural description of primitive groups. We recall a version of it below in Theorem 5.1. A proof of the Theorem can be found for example in **[LPS88]** or **[DM96, chapter 4]**.

Our version of this theorem splits the primitive permutation groups in five types. In the first type the socle of the primitive group is abelian and hence we do not need to consider this type for the purpose of the computation of maximal subgroups. However, we include this type in the list for completeness. The types 2 - 5 on the other hand have non-abelian socles and we will have to consider these types.

Theorem 5.1 (O'Nan-Scott). *Let G be a group which acts primitively and faithfully on Ω with $|\Omega| = n$. Let $H = \mathrm{Soc}(G)$ and $\omega \in \Omega$. Then H is homogeneous of type T and exactly one of the following cases holds.*

1. *"Affine". T is abelian of order p, $n = p^m$ and $\mathrm{Stab}_G(\omega)$ is a complement to H which acts irreducibly on H.*
2. *"Almost simple". $m = 1$ and $H \lhd G \leq \mathrm{Aut}(H)$.*
3. *"Diagonal type". $m \geq 2$ and $n = |T|^{m-1}$. Further, G is a subgroup of $V = (T \wr S_m).\mathrm{Out}(T) \leq \mathrm{Aut}(T) \wr S_m$ in diagonal action and either*
   a) *$m = 2$ and G acts intransitively on $\{T_1, T_2\}$ or*
   b) *$m \geq 2$ and G acts primitively on $\{T_1, \ldots, T_m\}$.*

   In case a) T_1 and T_2 both act regularly. Moreover, the point stabilizer V_ω of V is of the form $\mathrm{diag}(\mathrm{Aut}(T)^{\times m}).S_m \cong \mathrm{Aut}(T) \times S_m$ and thus $H_\omega = \mathrm{diag}(T^{\times m})$.
4. *"Product type". $m = rs$ with $s > 1$. We have that $G \leq W = A \wr B$ and the wreath product acts in product action with A acting primitively, but not regularly, on d points and B acting transitively on s points. Thus $n = d^s$. The group A is primitive of either*
   a) *type 3a with socle T^2 (i.e. $r = 2$, $s < m$),*
   b) *type 3b with socle T^r (i.e. $r > 1$, $s < m$) or*
   c) *type 2 (i.e. $r = 1$, $s = m$).*

   We have that $W_\omega \cap A^s \cong A_1^{\times s}$ and $\mathrm{Soc}(G) = \mathrm{Soc}(W)$. Furthermore $W = A^{\times s}G$.
5. *"Twisted wreath type". H acts regularly and $n = |T|^m$. G_ω is isomorphic to a transitive subgroup of S_m. The normalizer $N_{G_\omega}(T_1)$ has a composition factor isomorphic to T. Thus, in particular, $m \geq k+1$ where k is the smallest degree of a permutation group which has T as a composition factor.*

Proof. The case distinction and closer description of the different cases is proved in **[DM96, chapter 4]**. It remains to show that G is of exactly one of the types listed and cannot be listed under two different categories. In type 1 the socle is abelian, in type

5 the socle is nonabelian but regular; type 2 is the only type with a simple nonabelian socle. To distinguish type 3 from type 4, we observe that in type 3 the point stabilizer in H is a diagonal and thus simple, while in type 4 this point stabilizer is a direct product of point stabilizers of constituent groups and thus is not simple. Cases 3a and 3b are distinguished on whether the socle is a minimal normal subgroup. The three subcases of type 4 are distinguished by the action of the point stabilizer in the socle on its orbits. □

Remark 5.2. The labelling of types in the literature is inconsistent. The following table gives translations of the labellings used.

Type	1	2	3a	3b	4a	4b	4c	5
[DM96, Section 4.8]	i	iii	iv	iv	v	v	v	ii
[LPS88]	I	II	IIIa	IIIa	IIIb	IIIb	IIIb	IIIc
[Neu86]	I	V	II	III	II	III	IV	IV

Note that for case 3a/b) we change the case distinction of **[DM96, Theorem 4.5A]** from degree $2/>2$ to intransitive/primitive.

Remark 5.3. Type A in Theorem 4.2 corresponds to primitivity of type 2, 3b, 4b, 4c or 5. Type B corresponds to type 3a or 4a.

We now use Theorem 5.1 to determine primitive permutation representations of our given group G. We will need to answer the following questions for each of the types 2 - 5 of Theorem 5.1:

i) What extra conditions on G are necessary and sufficient for G to have a faithful primitive action of a certain type.

ii) If G has such an primitive action, then classify all these actions up to conjugacy of the point stabilizers in G and determine their point stabilizers.

For type 2 these questions are answered easily: A group G has faithful primitive representations of type 2 if and only if its socle is nonabelian simple. The classification of finite simple groups **[Gor82]** can be used to identify the socle T of G and then we can employ pre-tabulated results as well as parametrizations for some of the series to obtain the maximal subgroups of G. See **[Sax95]** for a recent survey.

Another approach to obtain the primitive permutation representations of an almost simple group is by using the data base of table of marks together with generator words for subgroup representatives, see **[Mer98]**. Such a data base is available in GAP, see **[GAP00]**. (In particular, such a data base can comprise all almost simple groups, for which computation of the full lattice would be still feasible.) However, to use this precomputed data, algorithms for the constructive recognition of almost simple groups are required. Much work has been done in this area recently, see for example **[BP00, CFL97, KS]**.

For types 3-5 the situation is more complex. Theorem **[Kov86, 4.3]** can give a parametrization of maximal subgroups of type 3 and 4 though we have not studied the feasibility of this approach. Similarly, **[Bad93]** describes groups of type 5 in more detail. However, the computation of complements to a nonsolvable normal subgroup might become a problematic subtask in this case.

A more detailed examination of whether a group can be primitive in one of these cases will be the subject of a subsequent study.

6. Runtime requirements

The solvable part of the algorithm requires the solvable radical. This can be obtained efficiently using the methods in **[LS97, Hol97]**. Then we need to construct the lower nilpotent series and Frattini subgroups for the nilpotent factors involved. A practical algorithm for this purpose is outlined in **[CLG]**. Furthermore, as one can consider these subgroups as O^{Σ}, for Σ the class of cyclic p-groups, **[KL90]** asserts that the calculation is possible in polynomial time.

For the computation of maximal subgroups we use the algorithms of **[LMR94]** and **[HLOR95]**. **[Rón90]** proves (for equivalent algorithms) that these calculations can be done in polynomial time.

The remaining steps for the computation of complements are linear algebra which is of polynomial time, provided the factor presentation is of polynomial length, which **[KS99]** assures.

An implementation of the solvable part of the algorithm shows that this method is highly efficient.

For the Fitting-free case we need to compute the action on chief factors. The required chief series, kernel, and intersections with normal subgroups again are in the polynomial time toolkit. Constructive recognition of the factor constituents **[KS]** then permits to write down a representation for the action of the chief factor(s).

We have not yet examined the determination of possible faithful primitive actions. However even for the almost simple case it seems impossible to give a general complexity, as we have to rely on pretabulated data (to get the maximal subgroups of almost simple groups) and we might only be able to bound the runtime by a function of the size of the involved simple groups and the width of the nonabelian composition factors.

7. Final comments

We have presented the algorithm for permutation groups. However – as with many other “hybrid” algorithms – the permutational group structure is only needed within

subtasks such as the computation of the solvable radical or a chief series. Once all these subproblems are solvable for a group in another representation, our algorithm becomes available immediately.

The authors would like to thank the referee for helpful comments.

Part of the work was undertaken while the second author was at the University of St Andrews, supported by EPSRC Grant GL/L21013.

References

[AB00] Christine Altseimer and Alexandre V. Borovik, *A non-deterministic algorithm for recognition of orthogonal and symplectic groups*, these proceedings.

[Bad93] R. W. Baddeley, *Primitive permutation groups with a regular nonabelian normal subgroup*, Proc. London Math. Soc. (3) **67** (1993), no. 3, 547–595.

[BGK+97] L. Babai, A. J. Goodman, W. M. Kantor, E.M. Luks, and P. P. Pálfy, *Short presentations for finite groups*, J. Algebra **194** (1997), 97–112.

[BP00] Sergey Bratus and Igor Pak, *Fast constructive recognition of a black box group isomorphic to S_n or A_n using Goldbach's conjecture*, J. Symbolic Comput. **29** (2000), 33–57

[Cam81] Peter J. Cameron, *Finite permutation groups and finite simple groups*, Bull. London Math. Soc. **13** (1981), 1–22.

[CCH] John Cannon, Bruce Cox, and Derek Holt, *Computing the subgroup lattice of a permutation group*, J. Symbolic Comput., to appear.

[CFL97] Gene Cooperman, Larry Finkelstein, and Steve Linton, *Constructive recognition of a black box group isomorphic to* $\mathrm{GL}(n,2)$, In Finkelstein and Kantor **[FK97]**, pp. 85–100.

[CH97] John Cannon and Derek Holt, *Computing chief series, composition series and socles in large permutation groups*, J. Symbolic Comput. **24** (1997), 285–301.

[CLG] John Cannon and Charles R. Leedham-Green, *Presentations of finite soluble groups*, in preparation.

[CNW90] Frank Celler, Joachim Neubüser, and Charles R. B. Wright, *Some remarks on the computation of complements and normalizers in soluble groups*, Acta Appl. Math. **21** (1990), 57–76.

[CS] John Cannon and Bernd Souvignier, *On the computation of normal subgroups in permutation groups*, Internat. J. Algebra Comput., to appear.

[CS97] John Cannon and Bernd Souvignier, *On the computation of conjugacy classes in permutation groups*, Proceedings of the 1997 International Symposium on Symbolic and Algebraic Computation (Wolfgang Küchlin, ed.), The Association for Computing Machinery, ACM Press, 1997, pp. 392–399.

[DM96] John D. Dixon and Brian Mortimer, *Permutation groups*, Graduate Texts in Mathematics, vol. 163, Springer, 1996.

[Eic97] Bettina Eick, *Special presentations for finite soluble groups and computing (pre-)Frattini subgroups*, In Finkelstein and Kantor **[FK97]**, pp. 101–112.

[EW] Bettina Eick and Charles Wright, *Computing formation-theoretic subgroups and certain complements in finite solvable groups*, In preparation.

[FK97] Larry Finkelstein and William M. Kantor (eds.), *Groups and computation II*, DIMACS: Series in Discrete Mathematics and Theoretical Computer Science, vol. 28, Providence, RI, Amer. Math. Soc., 1997.

[GAP00] The GAP Group, Aachen, St Andrews, GAP – *Groups, Algorithms, and Programming, Version 4.2*, 2000, (`http://www-gap.dcs.st-and.ac.uk/~gap`).

[Gor82] Daniel Gorenstein, *Finite simple groups*, Plenum Press, 1982.

[HLOR95] Derek F. Holt, Charles R. Leedham-Green, Eamonn A. O'Brien, and Sarah Rees, *Smash – matrix groups and G-modules*, 1995, A GAP share package.

[Hol00] Derek F. Holt, *Computing the automorphism group of a finite group*, these proceedings.

[Hol97] Derek F. Holt, *Representing quotients of permutation groups*, Quart. J. Math. Oxford Ser. (2) **48** (1997), no. 191, 347–350.

[Hul98] Alexander Hulpke, *Computing normal subgroups*, Proceedings of the 1998 International Symposium on Symbolic and Algebraic Computation (Oliver Gloor, ed.), The Association for Computing Machinery, ACM Press, 1998, pp. 194–198.

[Hul99a] Alexander Hulpke, *Computing subgroups invariant under a set of automorphisms*, J. Symbolic Comput. **27** (1999), no. 4, 415–427, (ID jsco.1998.0260).

[Hul99b] Alexander Hulpke, *Techniques for the computation of Galois groups*, Algorithmic Algebra and Number Theory (B. H. Matzat, G.-M. Greuel, and G. Hiss, eds.), Springer, 1999, pp. 65–77.

[Hul] Alexander Hulpke, *Conjugacy classes in finite permutation groups via homomorphic images*, Math. Comp., posted on May 24, 1999, PII: S 0025-5718(99)01157-6, (to appear in print).

[KL90] William M. Kantor and Eugene M. Luks, *Computing in quotient groups*, Proceedings of the 22nd ACM Symposium on Theory of Computing, Baltimore, ACM Press, 1990, pp. 524–563.

[Kov86] L. G. Kovács, *Maximal subgroups in composite finite groups*, J. Algebra **99** (1986), 114–131.

[KS] William M. Kantor and Ákos Seress, *Black box classical groups*, Mem. Amer. Math. Soc., Amer. Math. Soc., to appear.

[KS99] William M. Kantor and Ákos Seress, *Permutation group algorithms via black box recognition algorithms*, Groups St Andrews 1997 in Bath (C. M. Campbell, E. F. Robertson, N. Ruskuc, and G. C. Smith, eds.), London Mathematical Society Lecture Note Series, vol. 260/261, Cambridge University Press, 1999, pp. 436–

446.

[LMR94] Klaus Lux, Jürgen Müller, and Michael Ringe, *Peakword Condensation and Submodule Lattices: An Application of the Meat-Axe*, J. Symbolic Comput. **17** (1994), 529–544.

[LPS88] Martin W. Liebeck, Cheryl E. Praeger, and Jan Saxl, *On the O'Nan-Scott theorem for finite primitive permutation groups*, J. Austral. Math. Soc. Ser. A **44** (1988), 389–396.

[LS97] Eugene M. Luks and Ákos Seress, *Computing the fitting subgroup and solvable radical for small-base permutation groups in nearly linear time*, In Finkelstein and Kantor **[FK97]**, pp. 169–181.

[Mer98] Thomas Merkwitz, *Markentafeln endlicher Gruppen*, Diplomarbeit, Lehrstuhl D für Mathematik, Rheinisch-Westfälische Technische Hochschule, Aachen, 1998.

[Neu60] Joachim Neubüser, *Untersuchungen des Untergruppenverbandes endlicher Gruppen auf einer programmgesteuerten elektronischen Dualmaschine*, Numer. Math. **2** (1960), 280–292.

[Neu86] Peter M. Neumann, *Some algorithms for computing with finite permutation groups*, Groups – St Andrews 1985 (Edmund F. Robertson and Colin M. Campbell, eds.), Cambridge University Press, 1986, pp. 59–92.

[Rón90] Lajos Rónyai, *Computing the structure of finite algebras*, J. Symbolic Comput. **9** (1990), no. 3, 355–373.

[Sax95] Jan Saxl, *Finite simple groups and permutation groups*, Finite and locally finite groups (Istanbul, 1994), Kluwer Acad. Publ., Dordrecht, 1995, pp. 97–110.

[Sco80] Leonard L. Scott, *Representations in characteristic p*, The Santa Cruz conference on finite groups (Providence, RI) (Bruce Cooperstein and Geoffrey Mason, eds.), Proc. Sympos. Pure Math., vol. 37, Amer. Math. Soc., 1980, Corrigendum in **[LPS88]**, pp. 318–331.

[Sta73] Richard P. Stauduhar, *The determination of Galois groups*, Math. Comp. **27** (1973), 981–996.

Fachbereich 17, Universität Kassel,
Heinrich Plett Str. 40, 34132 Kassel, Germany
eick@mathematik.uni-kassel.de

Department of Mathematics, The Ohio State University
231 W 18th Avenue, Columbus, OH 43210, USA
ahulpke@math.ohio-state.edu